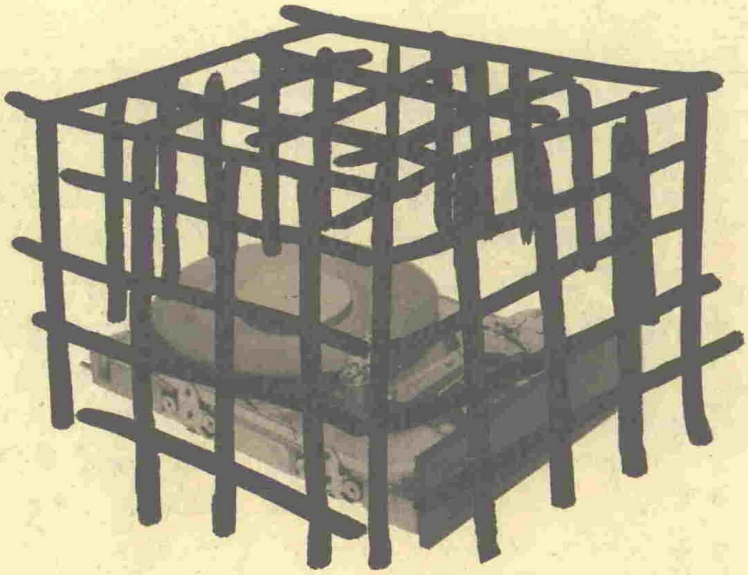
การจัดการฮาร์ดดิสค์ ให้ปลอดจากไวรัส



ยืน ภู่วรวรรณ

"บทความนี้เขียนขึ้นจากหลักการพื้นฐานของโปรแกรมจัดระบบงานเอ็มเอสดอส และความเป็นไปได้ของกลไกของไวรัสในปัจจุบัน เพื่อเสนอแนวทางให้ผู้ใช้งานฮาร์ดดิสค์มีโอกาสปลอดจากเชื้อไวรัสที่อาจแพร่เข้ามาหาได้"

ฮาร์ดดิสค์ อุปกรณ์ที่มีความจำเป็นของระบบงานปัจจุบัน

ข้อมูลและโปรแกรมเป็นสิ่งสำคัญของงานประมวลผลด้านคอมพิวเตอร์ ปัจจุบันผู้ใช้คอมพิวเตอร์มีความจำเป็นต้องเก็บข้อมูลจำนวนมากสำหรับการประมวลผลข้อมูล นอกจากนี้โปรแกรมคอมพิวเตอร์ประเภทโปรแกรมสำเร็จรูปก็มีขนาดใหญ่มาก ดังนั้น ความจำเป็นของการใช้ฮาร์ดดิสค์จะเพิ่มความสำคัญขึ้นเรื่อย ๆ หากคิดราคาของฮาร์ดดิสค์ต่อหน่วยการเก็บข้อมูล เมื่อเทียบกับฟลอปปี้ดิสค์แล้ว ราคาของฮาร์ดดิสค์จะเหมาะสมต่อการใช้งานมาก และนี่เองเป็นเหตุทำให้การใช้งานฮาร์ดดิสค์แพร่หลายเพิ่มขึ้นอย่างรวดเร็ว จนในปัจจุบันเครื่องไมโครคอมพิวเตอร์ที่ใช้งานกันทั่วไปมักมีฮาร์ดดิสค์ประกอบอยู่ด้วยเสมอ ฮาร์ดดิสค์จึงเป็นเสมือนที่เก็บของทั้งโปรแกรมและข้อมูล และที่เป็นปัญหาคือ ฮาร์ดดิสค์เป็นที่รวมของการใช้งานของผู้ใช้หลาย ๆ คน และนี่เองจึงเป็นการเสี่ยงอย่างมากที่ฮาร์ดดิสค์จะเป็นตัวรับเชื้อไวรัสและแพร่ขยายต่อออกไปยังแผ่นฟลอปปี้ดิสค์อื่น ๆ และขยายต่อไปยังเครื่องได้ไม่รู้จบ ลองนึกภาพดูว่า ถ้าในวันหนึ่งมีผู้ใช้ฮาร์ดดิสค์ร่วมกัน 10 คน และหนึ่งในนี้นำไวรัสมาแพร่ลงฮาร์ดดิสค์ ไวรัสก็อาจแพร่เข้าหาแผ่นดิสค์เกตต์ของคนที่เหลือทั้งหมดได้ และเมื่อนำไปใช้กับเครื่องอื่นอีกผลของการแพร่กระจายก็จะไม่มีที่สิ้นสุด

จะใช้ฮาร์ดดิสค์อย่างไรให้ปลอดภัย

ฮาร์ดดิสค์เป็นแหล่งที่ไวรัสจะเข้าไปได้ง่าย ดังนั้น เราจะต้องหาวิธีป้องกันไม่ให้ไวรัสเข้าไปในฮาร์ดดิสค์เป็นประการแรก เมื่อป้องกันเต็มที่แล้วไวรัสยังเข้าไปได้ เราก็ต้องหาวิธีการตรวจสอบให้ได้ว่ามีไวรัสบุกเข้ามาแล้ว และประการสุดท้ายก็คือการกำจัด ดังนั้น การใช้ฮาร์ดดิสค์ให้ปลอดภัยจึงต้องรู้จักกับ 3 วิธีของการจัดการไวรัส คือ **ป้องกัน ตรวจสอบ** และ **กำจัด**

ก่อนอื่นต้องเข้าใจโครงสร้างของฮาร์ดดิสค์

ฮาร์ดดิสค์ก็เหมือนดิสเกตต์ในแง่ลอจิคัล แต่ทางด้านฟิสิคัลจะต่างกันตรงที่ฮาร์ดดิสค์มีหลายแผ่นซ้อนกันที่เรียกว่า พื้นผิว และมีหัวอ่านหลายหัวอ่าน แต่ทางด้านลอจิคัลแล้วจะประกอบด้วยเซกเตอร์เก็บข้อมูล ในแต่ละเซกเตอร์เก็บข้อมูลได้ 512 ไบต์ หลายเซกเตอร์รวมกันเป็นกลุ่มเรียกว่า คลัสเตอร์ คลัสเตอร์หนึ่ง ๆ จะมีจำนวนเซกเตอร์เท่ากับจำนวนหัวอ่าน (โดยทั่วไป) การกำหนดตำแหน่งการเขียนข้อมูลจะบอกเป็นคลัสเตอร์ ดังนั้น ถึงต้องมีผังการจัดคลัสเตอร์ว่าใช้เก็บข้อมูลแล้วหรือยังที่เรียกว่า FAT (File Allocation Table) ดังนั้นไฟล์แต่ละไฟล์จะได้รับการกำหนดว่าเก็บข้อมูลไว้ในคลัสเตอร์ใดบ้างด้วยการบอกด้วย FAT นั่นเอง

โครงสร้างของการเก็บข้อมูลบนฮาร์ดดิสค์จะเป็นดังรูปที่ 1

ในฮาร์ดดิสค์แต่ละตัวประกอบด้วยเซกเตอร์ย่อยจำนวนมาก โดยเมื่อจัดเป็นคลัสเตอร์แล้วจะมีจำนวนสูงสุดเท่ากับคลัสเตอร์สูงสุดของฮาร์ดดิสค์นั้น ๆ ส่วนเก็บข้อมูลในเซกเตอร์แรกสุดเป็นที่เก็บข้อมูลที่เราเรียกว่า บูตเรคอร์ด (boot record) ข้อมูลส่วนนี้คือโปรแกรมที่จะทำหน้าที่โหลดโปรแกรมจัดระบบงาน (ส่วนนี้เป็นที่อยู่ของไวรัสบางตัว หรือเป็นตัวชี้ไปยังไวรัสบางตัวได้)

การเก็บข้อมูลในดิสค์จะเริ่มจากการใส่ชื่อไฟล์ลงในเซกเตอร์ไดเรคทอรี ส่วนการเก็บข้อมูลชื่อไฟล์เรียกว่า FCB (File Control Block) ส่วนไฟล์คอนโทรลบล็อกนี้รวมกันจะเป็นข้อมูลของไดเรคทอรีนั้น

ไฟล์คอนโทรลบล็อกเก็บข้อมูลไว้หลายอย่าง เช่น ข้อมูลเกี่ยวกับขนาด ชนิดของไฟล์ วันที่ เวลาของการปรับปรุงครั้งหลังสุด ตลอดจนตัวชี้ไปยังจุดเริ่มต้นของตาราง FAT ซึ่งจะชี้เชื่อมต่อไปยังตารางลำดับต่อไปเรื่อย ๆ จนจบไฟล์

ลักษณะของการเก็บข้อมูลจึงเก็บเรียงจากคลัสเตอร์ต้น ๆ ลงไปเรื่อย ๆ นอกเสียจากมีการลบจะเกิดคลัสเตอร์ว่างเพื่อให้ใช้งานได้ใหม่

แบ่งไดเรคทอรีย่อยข้อมูลและโปรแกรมออกจากกัน

เมื่อทำการฟอร์แมตฮาร์ดดิสค์เรียบร้อยแล้ว ควรวางแผนการใช้ฮาร์ดดิสค์ โดยการแบ่งแยกเป็นไดเรคทอรีย่อย สิ่งที่สำคัญคือต้องแยกโปรแกรมใช้งานกับข้อมูลออกจากกัน ส่วนของโปรแกรมเป็นส่วนที่ยอมให้ใช้งานร่วมกันได้ แต่ส่วนของข้อมูลต้องแยกผู้ใช้แต่ละคนออกจากกัน และให้แต่ละผู้ใช้คอยดูแลข้อมูลของตนเอง ดังนั้นหากพบว่าข้อมูลอื่นแปลกปลอมมาในไดเรคทอรีย่อยของตนเองมีสิทธิ์ลบทิ้งได้

ตัวอย่างเช่น ในสำนักงานแห่งหนึ่งมีผู้ใช้ 4 คน คือ A, B, C และ D งานหลักที่ใช้มีทั้ง ดาต้าเบส สเปรดชีต เวิร์ดโปรเซสเซอร์ และกราฟิก เราสามารถจัดการฮาร์ดดิสค์ออกเป็นไดเรคทอรีย่อยได้ดังรูปที่ 2

ในการแบ่งแยกเป็นไดเรคทอรีย่อยนี้ จะต้องเน้นให้ผู้ใช้งานทุกคนทำตามโดยไม่เข้ามาก้าวก่ายในส่วนของผู้อื่น สิ่งที่จะต้องกระทำคือการสร้างไดเรคทอรีย่อยและการเข้าสู่ไดเรคทอรีย่อย ผู้ใช้ทุกคนจะต้องมีความรู้พื้นฐานเหล่านี้

บนฮาร์ดดิสค์จะมีโปรแกรม AUTOEXEC.BAT ที่กำหนด PATH ไว้ ข้อสำคัญคือ เครื่องที่มีฮาร์ดดิสค์จะต้องบูตผ่านจากฮาร์ดดิสค์เสมอ ห้ามบูตด้วยดิสค์ไดรฟ์ A โดยเด็ดขาด การกำหนด PATH เราทำในไฟล์ AUTOEXEC.BAT ดังนี้

```
AUTOEXEC.BAT มีข้อมูล
CLS
FILES   = 20
BUFFERS = 12
PATH    = C:\LOTUS;C:\DBASE;
          C:\WP5;C:\HG
```

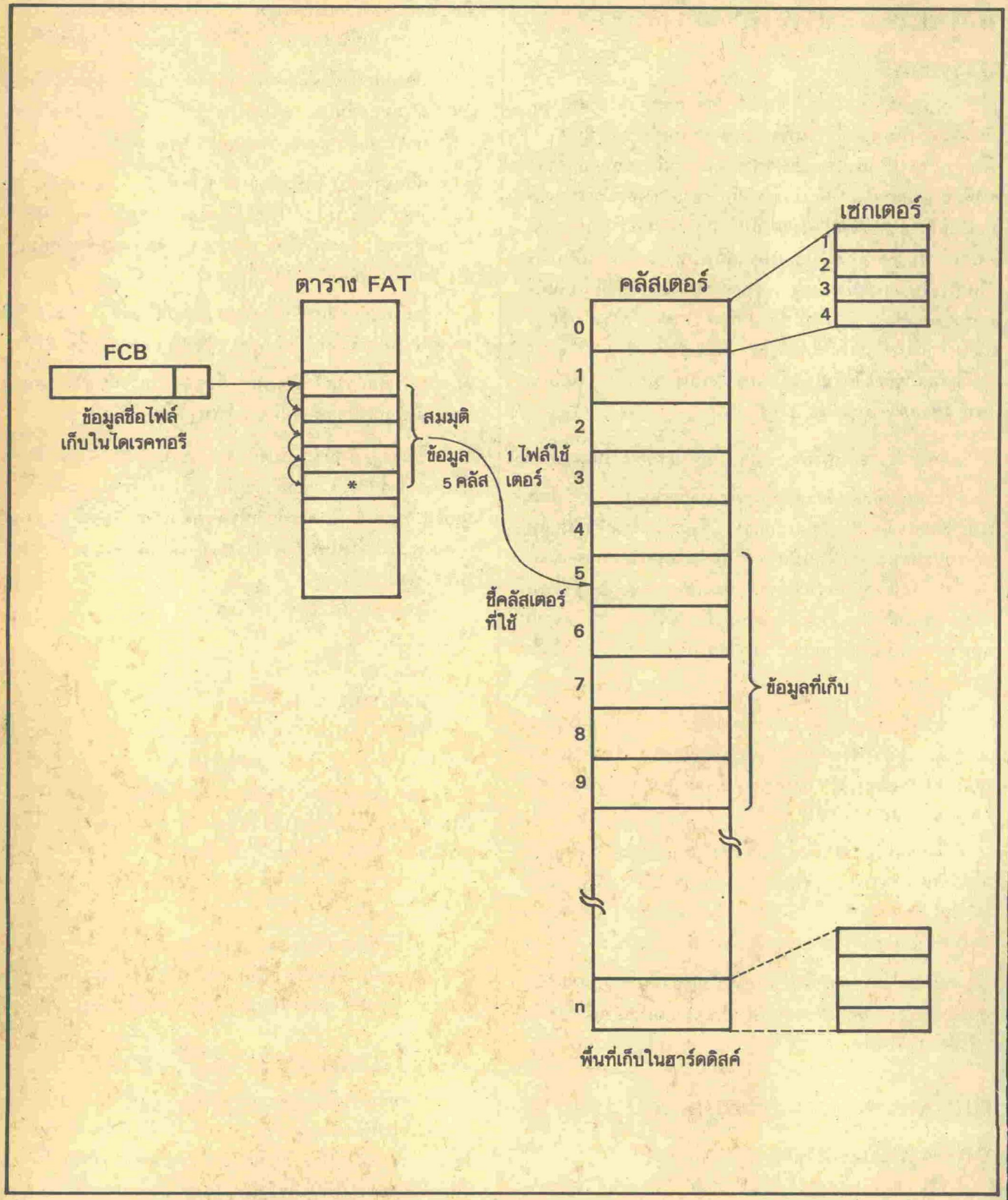
ในการกำหนด PATH นี้จะทำให้ผู้ใช้สามารถเรียกโปรแกรมจากไดเรคทอรีของตนเองได้ เช่น เมื่อผู้ใช้ A จะใช้งานโลตัส ผู้ใช้A จะต้องปฏิบัติ ดังนี้

```
C > CD A
C > LOTUS
```

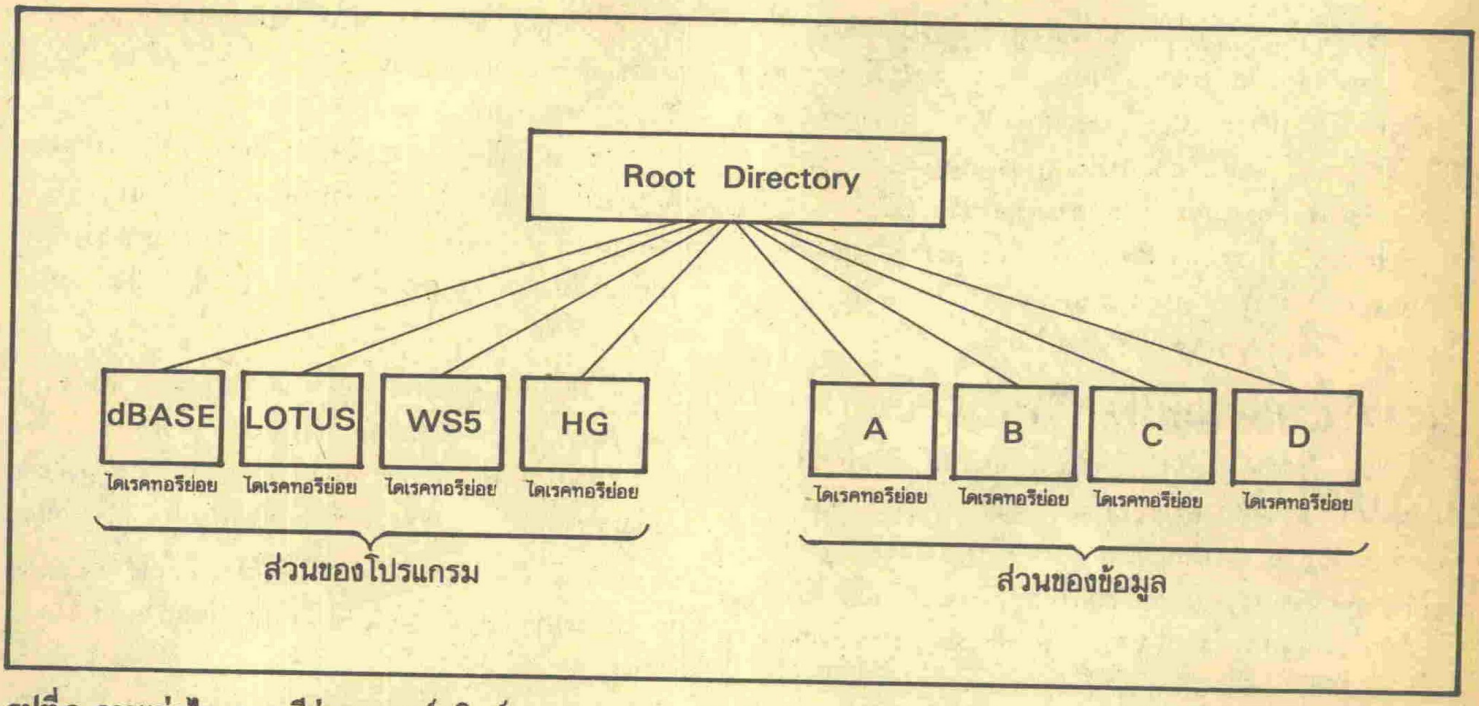
การเรียกจากไดเรคทอรีของตนเองนี้สามารถเข้าใช้โปรแกรมที่กำหนด PATH ไว้ได้หมด เมื่อใช้ในไดเรคทอรีของตนเอง การสร้างแฟ้มข้อมูลก็จะเกิดขึ้นไม่ไปปะปนกับผู้อื่น

ให้ใช้โปรแกรม .EXE ในฮาร์ดดิสค์

การเรียกใช้โปรแกรมสำเร็จรูปต่าง ๆ หรือโปรแกรม .EXE นั้นให้เรียกจากที่เก็บไว้ในฮาร์ดดิสค์ ดังนั้น ถ้าต้องการใช้โปรแกรมอะไรให้นำโปรแกรมนั้นมาเก็บในฮาร์ดดิสค์ ก่อนเก็บให้ตรวจสอบให้มั่นใจว่าไม่มีไวรัสแปลกปลอมเข้ามา แล้วเก็บไว้ในฮาร์ดดิสค์ในไดเรคทอรีย่อยที่สร้างขึ้น จากนั้นสร้าง



รูปที่ 1 โครงสร้างการเก็บข้อมูลลงบนฮาร์ดดิสค์



รูปที่ 2 การแบ่งไดเรคทอรีย่อยบนฮาร์ดดิสค์

PATH ให้ไปยังไดเรคทอรี่ย่อยนั้นได้ โปรแกรมที่จำเป็น เช่น โปรแกรมในกลุ่มของ DOS UTILITY โปรแกรมใช้งานเฉพาะการดูแลเครื่อง เช่น Norton Utility หรือ PC Tools อย่าลืมว่าควรเน้นให้ใช้ .EXE บนฮาร์ดดิสค์เท่านั้น

การเก็บข้อมูลสำรองเป็นเรื่องสำคัญ

ในการใช้ฮาร์ดดิสค์นั้นมีข้อพึงปฏิบัติในเรื่องการสำรองข้อมูลอย่างยิ่ง ผู้ไม่ประมาทจะต้องทำการสำรองโดยสม่ำเสมอ การสำรองข้อมูลเป็นวิธีการที่ทำให้ปลอดภัยจากการเสียหายของของข้อมูลบนฮาร์ดดิสค์ไม่ว่าจะด้วยจากเหตุการณ์ใดก็ตาม

การสำรองควรทำการสำรองทั้ง 2 รูปแบบ คือ สำรองตัวโปรแกรมและข้อมูลสำหรับตัวโปรแกรมนั้น จะเก็บแผ่นต้นฉบับไว้ แล้วติดป้องกันการเขียนอย่างดี ตัวโปรแกรมจะต้องเก็บรักษาไว้โดยไม่ให้ผู้ใดมาแกะแผ่นสติกเกอร์ป้องกันการเขียนแล้วไปใช้ที่อื่นโดยเด็ดขาด

สำหรับการสำรองข้อมูลควรทำสม่ำเสมอ และที่สำคัญทำให้ง่ายต่อการดำเนินการ เช่น เขียนโปรแกรมใน .BAT ไว้ เช่น ไฟล์ BACK.BAT มีคำสั่งดังต่อไปนี้

```
COPY C:/WIPA/MYDATA.DBF A:
COPY C:/WIPA/SALES.WK1   A:
  :
```

หากต้องการสำรองแฟ้มข้อมูลขนาดใหญ่มาก เช่น แฟ้มข้อมูลใน .dbf ที่มีข้อมูลจำนวนมากกว่าดิสเกตต์หนึ่งแผ่น เราจะต้องทำการสำรองข้อมูลโดยใช้คำสั่ง BACKUP ที่เป็น DOS Utility ดังนี้

```
BACKUP C : * .DBF A : /S/M/A/D : :20-08-88
```

/S หมายถึงนำเอาข้อมูลในไดเรคทอรีย่อยขึ้นมาด้วย

/M หมายถึงการสำรองเฉพาะ last update เท่านั้น

/A ให้ทำเฉพาะที่มีชื่อแล้วในแผ่น backup เดิมเท่านั้น

/D ให้ทำเฉพาะไฟล์ที่มีวันที่ = หรือมากกว่าที่กำหนด

การตรวจสอบสิ่งแปลกปลอมในฮาร์ดดิสค์

ในฮาร์ดดิสค์ประกอบด้วยข้อมูลจำนวนมากทำให้ยากต่อการตรวจสอบสิ่งแปลกปลอม วิธีที่ดีที่สุดที่อยากจะแนะนำคือ การพิมพ์ชื่อไฟล์ในไดเรคทอรีของร่วมหรือส่วนโปรแกรมเอาไว้ เช่น ไฟล์ในไดเรคทอรีดีเบสมี 28 ไฟล์ แต่ละไฟล์มีขนาดเท่าไร การเก็บข้อมูลเหล่านี้เอาไว้จะช่วยทำให้เราสามารถตรวจสอบได้ว่า ไดเรคทอรีโปรแกรมนั้นมีไฟล์อะไรเพิ่มเข้ามาเราจะได้ลบทิ้งได้ หรือไฟล์ใดมีขนาดเปลี่ยนแปลงไปจากเดิม เปลี่ยนแปลงไปเพราะอะไร ก็จะทราบได้

เปลี่ยนไฟล์ .EXE ในฮาร์ดดิสค์ให้เป็น Read only

โดยธรรมชาติของไวรัสที่จะเกาะแทรกไปกับ .EXE

ไฟล์นั้นจะต้องมีการเขียนข้อมูลเพิ่มลงไปใน .EXE ดังนั้น ถ้าโปรแกรมหลักของการทำงาน เช่น โปรแกรมในดีเบสและโลตัสนั้น เราสามารถเปลี่ยนไฟล์แอตทริบิวต์ให้อยู่ในรูปอ่านได้อย่างเดียวจะเขียนหรือลบไม่ได้ การทำเช่นนี้จะทำให้ไฟล์ .EXE ของเราปลอดภัยจากการเกาะของไวรัสได้

การเปลี่ยนแอตทริบิวต์ของไฟล์นั้น ทำได้ด้วยการใช้โปรแกรมยูทิลิตี้เข้าช่วย โปรแกรมยูทิลิตี้เหล่านี้มีหลายโปรแกรมในกลุ่ม Norton Utility โปรแกรมในกลุ่ม PC Tools

สร้างโปรแกรมแบตช์ไฟล์ทำเมนู

ในการใช้ฮาร์ดดิสก์มีวิธีการสร้างเมนูให้ผู้ใช้เลือกใช้งานในระดับ DOS ได้หลายรูปแบบ เช่น ใช้แบตช์ไฟล์สร้างเมนูให้ผู้ใช้เลือกใช้ตามไดเรคทอรีย่อย การเลือกตามเมนูนี้ผู้เขียนสามารถสร้างขึ้นมาตามความต้องการได้ ลักษณะของแบตช์ไฟล์จะประกอบด้วยคำสั่ง TYPE เพื่อส่งข้อความขึ้นจอภาพ และเมื่อผู้เลือกข้อใด ก็กดหมายเลข ตัวเลขเหล่านี้จะเป็นชื่อแบตช์ไฟล์เพื่อทำการเข้าสู่ไดเรคทอรีย่อยและทำงานตามที่ต้องการ เช่น ใน AUTOEXEC.BAT ประกอบด้วยคำสั่ง

```
CLS
FILES   = 20
BUFFER = 12
PATH = C: \ LOTUS;C: \ DBASE;C: \ WP5...
TYPE MENU.TXT
PROMPT $N$G
```

ในแฟ้ม MENU.TXT มีข้อความเป็นแฟ้มเอกสารเพื่อพิมพ์แสดงรายการเมนูบนจอภาพ

ถ้าหากให้ผู้ใช้ป้อนข้อมูลตามหัวข้อที่เลือก เช่น เลือกข้อ 1....10 ก็จะมีแบตช์ไฟล์จาก 1. bat, 2. bat... 10. bat ซึ่งในแต่ละแบตช์ไฟล์จะมีคำสั่งในการทำงานตามไดเรคทอรีย่อยที่กำหนด เช่น 1. bat เป็นของผู้ใช้ชื่อ WIPA ในแฟ้มนี้ก็จะมีคำสั่ง

```
CD WIPA
LOTUS
CD \
AUTOEXEC
```

การสร้างแบตช์ไฟล์นี้เป็นวิธีการควบคุมผู้ใช้ให้อยู่ในไดเรคทอรีของตนไม่ให้ไปสร้างข้อมูลไว้ในไดเรคทอรีอื่น ซึ่งจะทำให้การควบคุมทำได้ง่ายขึ้น

หาโปรแกรม data security มาใช้

ปัจจุบันมีผู้พัฒนาโปรแกรมควบคุมฮาร์ดดิสก์กันขึ้นมาใช้หลายโปรแกรม แต่ละโปรแกรมได้รับการพัฒนามาอย่างดียิ่ง ในที่นี้ขอแนะนำโปรแกรม Watchdog โปรแกรม Watchdog มีขีดความสามารถที่ผู้ใช้จะตั้งระบบได้มากมาย เช่น

- กำหนดการจัดการฮาร์ดดิสก์ด้วยการเข้าสู่ฮาร์ดดิสก์โดยการตั้งรหัสผ่าน ผู้รู้รหัสผ่านเท่านั้นจะเป็นผู้เข้าไปใช้ในฮาร์ดดิสก์ได้ ส่วนของรหัสผ่านจะได้รับการป้องกันไม่ให้การอ่านด้วยวิธีปกติได้เลย การบูตจะบูตจากไดรฟ์ A ก็ไม่สามารถเข้าสู่ฮาร์ดดิสก์ได้

- กำหนดพื้นที่สำหรับผู้ใช้งานต่าง ๆ กัน โปรแกรม Watchdog สามารถตั้งพื้นที่บนฮาร์ดดิสก์ โดยแต่ละพื้นที่จะยอมให้ userid ใด userid หนึ่งเข้ามาใช้ได้เท่านั้น ผู้ที่ตอบ userid ต่างออกไปไม่สามารถเข้ามาใช้ในพื้นที่หวงห้ามได้เลย

- ติดตั้งเมนูและเมนูย่อย เพื่อให้ผู้ใช้เลือกเข้าไปใช้งานในส่วนต่าง ๆ และติดตั้งเพิ่มเติมเมนู หรือแก้ไขเมนูได้ตามต้องการ

- บันทึกการใช้งานของผู้ใช้ไว้เพื่อให้ตรวจสอบได้ ดังนั้นจึงเป็นข้อเด่นที่จะตรวจสอบว่ามีผู้ใดใช้คอมพิวเตอร์บ้าง ใช้เมื่อไร ข้อมูลที่บันทึกไว้นี้สามารถสร้างเป็นรายงานได้

- มีตู้เมล์สำหรับการส่งข้อมูลข้าม Userid กัน เช่น ต้องการฝากข้อความถึงใครก็จะใส่ในตู้เมล์ของผู้นั้น เมื่อผู้นั้น log on ใช้งานก็ทราบว่ามีผู้ฝากข้อความไว้ก็สามารถเรียกออกมาดูได้

การใช้โปรแกรมจำพวก data security นี้ สามารถทำให้ไฟล์บางไฟล์อยู่ในสภาพ read only คืออ่านได้อย่างเดียว ไม่สามารถเขียนทับได้ ดังนั้น การป้องกันไวรัสในกรณีนี้อย่างเป็นไปได้ ผู้ใช้สามารถกำหนดพื้นที่ต่าง ๆ ไว้ให้ผู้ใช้เลือกใช้ตามความต้องการได้ โปรแกรมเหล่านี้เป็นโปรแกรมที่น่าใช้งานและมีประโยชน์ในยุคสมัยนี้มาก

ใช้โปรแกรมป้องกันไวรัส

สืบเนื่องจากปัญหาไวรัสเป็นปัญหาที่รุนแรงเพิ่มขึ้น จึงมีผู้พัฒนาโปรแกรมไวรัสขึ้นเพื่อการค้าก็มี เพื่อเป็นสมบัติสาธารณะก็มี ในต่างประเทศมีโปรแกรมหนึ่งชื่อ corporate ส่วนโปรแกรมในประเทศไทยที่พัฒนาขึ้นมาก็มีมาก เช่น โปรแกรมศิริราช โปรแกรมวัคซีนของการไฟฟ้าฝ่ายผลิต หรือ EGAT VACCINE โปรแกรมเหล่านี้มีความสามารถในการตรวจสอบไวรัสและแก้ปัญหาได้ดี

ผู้เขียนขอเล่าถึงขีดความสามารถของโปรแกรมป้องกันไวรัสทั่วไปว่าจะช่วยป้องกันได้อย่างไร การป้องกันมีหลายอย่าง

เช่น โปรแกรมวัคซีนนี้จะได้รับการโหลดเป็นโปรแกรมแบบ resident ไว้ในหน่วยความจำก่อน จากนั้นเราสามารถตั้งโปรแกรมให้คอยตรวจสอบดูกลุ่มของโปรแกรม .COM หรือ .EXE ว่ามีการเขียนลงไปหรือไม่ ถ้ามีการเขียนก็จะมีข้อความเตือนและถามเราว่ายินดีให้เขียนลงใน .EXE หรือ .COM นั้นหรือไม่ ถ้าไม่ยินดี โปรแกรมก็จะป้องกันไม่ให้มีการเขียน นอกจากนี้ยังคอยตรวจสอบลักษณะของไวรัสที่รู้จักว่ามีแฝงอยู่ที่ใดหรือไม่ และจะเตือนถ้าพบ

โปรแกรมป้องกันไวรัสบางตัวใช้วิธีการเขียนรหัสตรวจสอบจำนวนไบต์ของแต่ละไฟล์ไว้ในฮาร์ดดิสก์ การตรวจสอบจะใช้หลักการของ CRC ทำการตรวจสอบ ถ้าข้อมูลในไฟล์ใดไฟล์หนึ่งเปลี่ยนแปลงไป ก็จะตรวจสอบได้

โปรแกรมป้องกันไวรัสนี้มีข้อเสียคือ จะทำให้การทำงานโดยรวมของระบบเสียเวลามากขึ้น แต่มีบางโปรแกรมใช้สำหรับการตรวจสอบอย่างเดียว กรณีนี้จะใช้เฉพาะเมื่อจำเป็นเท่านั้น โปรแกรมเหล่านี้จะไม่เก็บไว้ในหน่วยความจำ

โปรแกรมป้องกันไวรัสทั่วไปที่เป็นโปรแกรมประเภทฝังตัวในหน่วยความจำ ส่วนใหญ่จะทำการตรวจสอบกลไกการทำงานดังนี้

- ตรวจสอบการเขียนแฟ้มประเภท .COM
- ตรวจสอบการเขียนแฟ้มประเภท .EXE
- ตรวจสอบการเขียนแฟ้ม COMMAND.COM
- ตรวจสอบการเขียนทับลงในบูตเซกเตอร์
- ตรวจสอบการเขียนทับลงใน FAT
- ตรวจสอบการโหลดโปรแกรมประเภทฝังตัวในหน่วยความจำ

ทั้งนี้เพราะไวรัสส่วนใหญ่มักจะใช้จุดเหล่านี้สำหรับการสร้างไวรัส อย่างไรก็ตาม โปรแกรมป้องกันก็ไม่สามารถป้องกันได้ร้อยเปอร์เซ็นต์

หากพบไวรัสจริง ๆ จะทำอย่างไร

ก่อนอื่นอย่ากังวลหรือตกใจใด ๆ ให้หาโปรแกรมวัคซีนเท่าที่หาได้ตรวจสอบและทำการแก้ไข ที่สำคัญคือโปรแกรมวัคซีนเหล่านั้นควรจะติดแถบสติกเกอร์ป้องกันการเขียนไว้ด้วย เมื่อตรวจสอบและแก้ไขได้ ก็จัดการเท่าที่จะทำได้

สำหรับผู้ที่ไม่มีความรู้ในเรื่องไวรัสมากก็ไม่ต้องกังวล ไวรัสส่วนใหญ่จะเกาะอยู่กับโปรแกรม .EXE หรือ .COM หรือฝังตัวอยู่ในดิสก์หรือโอเอส ทางที่ดีให้บูตจากแผ่น DOS ที่ติดป้องกันการเขียนและมั่นใจว่าไม่มีไวรัสจากนั้นใช้โปรแกรม COPY ของ DOS ทำการสำเนาข้อมูลทั้งหมดมาไว้ก่อน สำหรับตัวโปรแกรม .EXE และ .COM นั้น ถ้าเก็บสำเนาตามที่กล่าวแล้วในตอนต้นก็ไม่ต้องไปทำอะไร เพราะสามารถโหลดของใหม่ลงไปทับได้

ถ้ารู้ว่าไวรัสอยู่ที่ใด หรืออยู่ไฟล์ใด ให้ลบไฟล์นั้นทิ้งไปเสีย แล้วคัดลอกของใหม่ลงไป แต่ถ้าไม่แน่ใจว่าไวรัสติดอยู่ที่ใด ให้ทำการฟอร์แมตฮาร์ดดิสก์ใหม่ โดยเรามีสำเนาของ .EXE, .COM ไว้แล้ว ส่วนข้อมูลเราก็มีสำเนาแล้ว การฟอร์แมตฮาร์ดดิสก์ดูจะเป็นเรื่องยาก แต่เป็นวิธีที่แก้ปัญหาอย่างได้ผลมาก จะทำได้ก็ต้องมีการสำเนาข้อมูลอย่างมีระบบตามที่กล่าวแล้ว

การระมัดระวังเป็นเรื่องที่ปลอดภัย

หากการใช้งานประจำในสำนักงานมีการระมัดระวังและคอยตรวจสอบดูเป็นระยะ ก็คาดได้ว่าปัญหาไวรัสไม่น่าจะเกิดขึ้น หากเป็นเครื่องที่มีฮาร์ดดิสก์และใช้งานกันหลายคนจนยากที่จะควบคุมได้ อาจจะมีผู้นำเอาโปรแกรมต่าง ๆ มาทดลองหรือใช้งานปะปนอยู่ นับว่าเป็นเรื่องเสี่ยงต่อการติดไวรัสมาก การระมัดระวังเป็นสิ่งที่ปลอดภัยเสมอ

ส่งท้าย

หากผู้ใช้สนใจและหาทางเรียนรู้เทคนิคต่าง ๆ เกี่ยวกับคอมพิวเตอร์ไว้บ้าง เช่น เรียนรู้การใช้ยูทิลิตี้ต่าง ๆ เช่น Norton หรือ PC Tools ก็นับว่าเป็นเรื่องที่ดี เพราะอาจช่วยเหลือตัวเองได้ในบางโอกาส อย่างไรก็ตาม จะต้องรู้จริงและจะไม่ทำการทดลองใด ๆ โดยที่ไม่รู้จริงบนฮาร์ดดิสก์ โอกาสพลาดและมีปัญหาเกิดขึ้นเสมอสำหรับผู้ที่ลองของโดยไม่รู้จริง

ไวรัสเป็นสิ่งที่มนุษย์สร้างขึ้น ไวรัสไม่ใช่เรื่องใหญ่ การปฏิบัติตนเองในการใช้คอมพิวเตอร์อย่างมีหลักการจะเอาชนะไวรัสได้ไม่ยาก

ขอให้ผู้ใช้คอมพิวเตอร์ทั่วไปโชคดีและมีความสุขกับการใช้คอมพิวเตอร์ สวัสดีครับ!